UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,000	05/14/2001	Kilian schuster	132702-0033	1245

50659 7590 03/19/2007

BUTZEL LONG
STONERIDGE WEST
41000 WOODWARD AVENUE
BLOOMFIELD HILLS, MI 48304

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/855,000	SCHUSTER ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-31* is/are pending in the application.

4a) Of the above claim(s) *1-20* is/are ~~withdrawn from consideration~~. Canceled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21-31 are pending.

Claims 1-20 have previously been cancelled.

2. Claims 21-31 have overcome the rejection under 35 U.S.C. 101.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/29/2006 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 21-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky, et al. (US 6,421,453) and further in view of An, et al. (US 6,715,073).

As per claim 21:

Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure; **[col.1, lines 49-52 and col.8, lines 5-12]**

b. defining at least one requirement for the procedure; **[col.1, lines 52-56 and col.12, lines 37-48]**

c. defining at least one person to be authorized **[col.1, lines 57-63]** to perform the procedure; **[col.5, lines 12-30 and col.12, lines 37-40]**

d. detecting the occurrence of the at least one initiating event; **[col.1, lines 65-67 and col.9, lines 1-3]**

e. generating a virtual key **[col.3, lines 29-67 col.17, lines 57-58]** for the at least one based on the at least one requirement detecting the occurrence of the at least one

initiating event and prior to the at least one person arriving at the building; **[col.3, lines 30-32 and col.17, lines 5-7]**

f. transmitting virtual key to the at least one person; **[col.17, lines 5-7 and 59-60]**

g. detecting use of the virtual key; **[col.9, lines 64-66 and col.16, lines 64-66]**

h. checking the validity of the virtual key; and **[col.5, lines 39-43 and col.12, lines 42-48]**

i. initiating said procedure within the building if the validity check is positive. **[col.4, lines 61-66 and col.15, lines 40-46]**

j. performing said steps a. through i. in an access control computer system associated with the building. **[col.3, lines 28-30 and col.4, lines 61-63]**

Kanevsky discloses initiating event, which can broadly be given as the presence of a user attempting to access a facility, building, or vehicle/boat (col.13, lines 54-60). A requirement broadly interprets as any kind of security tasks that involves authorization or verification process necessary for (the procedure) gaining access to the facility (initiating event). Kanevsky discloses the claimed requirement refers to security tasks or user recognition (classification, identification, and verification) where this may involve interacting with the system to gain access (col.1, lines 35-36 and 49-51). In addition, Kanevsky includes a password verification as claimed the requirement for the procedure (to access) to the facility (initiating event) by using a gesture pin or password (virtual key) suggesting proof of possession in order to gain access (col.5, lines 3-10 and 40-42). Kanevsky discloses the password includes a sequence of intentionally performed gestures is referred to as gesture pins (col.5, lines 5-10 and 38-42). The virtual key can

obviously be Kanevsky's password (or gesture pin) that is used to verify the person or user to gain access to the building or facilities (col.5, lines 40-43 and col.8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col.17, lines 5-7). Therefore, the gesture pin is transmitted to the user for use to access the facility/service prompting checking the validity of the gesture pin (col.15, lines 41-47 and 18, lines 8-24). So depending on the security task(s) involved and the results of the user evaluation, the user is either granted/denied access to a service/facility or confirmed/denied with respect to ownership of an item (proof of possession, or information pertaining to the user's biometrics will be stored in a user database for different applications (col.8, lines 5-12 and col.12, lines 37-48). However, Kanevsky does not specifically disclose a password refers to a virtual key.

Hence, An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that authenticates a user (col.1, lines 43-48 and col.2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (to facilities/services).

As per claim 22: **See An on col.1, lines 64-col.2, line 1;** discusses a step of assigning an encrypted code to the virtual key.

As per claim 23: **See An on col.2, lines 5-12;** discusses the steps of adding a signature to the virtual key and identifying a recipient of the transmitted virtual key by the signature.

As per claim 24: **See Kanevsky on col.1, lines 49-55;** discusses defining different procedures for different initiating events.

As per claim 25: **See Kanevsky on col.13, lines 59-62 and col.29-53;** discusses defining different requirements for different procedures.

As per claim 26: See Kanevsky on col.9, lines 25-27 and An on col.1, lines 64-col.2, line 12; discusses transmitting different virtual keys to said person for different initiating events.

As per claim 27: See Kanevsky on col.17, lines 20-30; discusses storing said virtual key partially or completely.

As per claim 28: **See Kanevsky on col.17, lines 20-30;** discusses the steps of identifying the at least one person with biometrics characteristics.

As per claim 29:

method according to Claim 21, further comprising at least one of the steps of:

initiating a control procedure of an elevator in the building;

initiating a medical assistance procedure;

initiating a building cleaning procedure; and initiating a guest reception procedure.

Kanevsky discloses classification involves the differentiation of multiple individuals attempting to interact with the system and a purpose of identifying the individuals from their respective commands (col.1, lines 49-58 and col.5, lines 3-17). Kanevsky discusses that it is desirable to implement an extension of the identification task where the individuals attempting to interface with the computer are ranked so that a higher ranking individual (i.e. supervisor) is allowed access over a lower ranked individual (i.e. data entry person) (col.1, line 65-col.2, line 1). Further, Kanevsky discloses an apparatus/procedure for obtaining access to a computer/facility/service via the utilization of gesture pins (col.15, lines 29-32). Thus, it would have been obvious the computer/facility/service is referring to initiating a variety of procedures (i.e. an elevator in a building, medical assistance, building cleaning procedure or guest reception) that includes security tasks for different users to access to different services/facilities.

As per claim 30: **See col.31, lines 63-64;** discusses the step of transmitting the virtual key using wireless devices.

As per claim 31: New

Method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure; **[col.1, lines 49-52 and col.8, lines 5-12]**

b. defining at least one of a security requirement and an availability requirement for the procedure; **[col.1, lines 52-56 and col.12, lines 37-48]**

c. defining at least one person to be authorized **[col.1, lines 57-63]** to perform the procedure; **[col.5, lines 12-30 and col.12, lines 37-40]**

d. detecting the occurrence of the at least one initiating event; **[col.1, lines 65-67 and col.9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col.1, lines 16-22)]**

e. generating a virtual key **[col.3, lines 29-67 col.17, lines 57-58]** for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; **[col.3, lines 30-32 and col.17, lines 5-7]**

f. transmitting virtual key to the at least one person; **[col.17, lines 5-7 and 59-60]**

g. detecting use of the virtual key; **[col.9, lines 64-66 and col.16, lines 64-66]**

h. checking the validity of the virtual key; and **[col.5, lines 39-43 and col.12, lines 42-48]**

i. initiating said procedure within the building if the validity check is positive. **[col.4, lines 61-66 and col.15, lines 40-46]**

j. performing said steps a. through i. in an access control computer system associated with the building. **[col.3, lines 28-30 and col.4, lines 61-63]**

Kanevsky discloses initiating event, which can broadly be given as the presence of a user attempting to access a facility, building, or vehicle/boat (col.13, lines 54-60). A requirement broadly interprets as any kind of security tasks that involves authorization or verification process necessary for (the procedure) gaining access to the facility (initiating event). Kanevsky discloses the claimed requirement refers to security tasks

or user recognition (classification, identification, and verification) where this may involve interacting with the system to gain access (col.1, lines 35-36 and 49-51). In addition, Kanevsky includes a password verification as claimed the requirement for the procedure (to access) to the facility (initiating event) by using a gesture pin or password (virtual key) suggesting proof of possession in order to gain access (col.5, lines 3-10 and 40-42). Kanevsky discloses the password includes a sequence of intentionally performed gestures is referred to as gesture pins (col.5, lines 5-10 and 38-42). The virtual key can obviously be Kanevsky's password (or gesture pin) that is used to verify the person or user to gain access to the building or facilities (col.5, lines 40-43 and col.8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col.17, lines 5-7). Therefore, the gesture pin is transmitted to the user for use to access the facility/service prompting checking the validity of the gesture pin (col.15, lines 41-47 and 18, lines 8-24). So depending on the security task(s) involved and the results of the user evaluation, the user is either granted/denied access to a service/facility or confirmed/denied with respect to ownership of an item (proof of possession, or information pertaining to the user's biometrics will be stored in a user database for different applications (col.8, lines 5-12 and col.12, lines 37-48). However, Kanevsky does not specifically disclose a password refers to a virtual key.

Hence, An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that

authenticates a user (col.1, lines 43-48 and col.2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (to facilities/services).

Response to Arguments

6. Applicant's arguments filed 12/29/2006 have been fully considered but they are not persuasive.

Kanevsky discloses the password includes a sequence of intentionally performed gestures is referred to as gesture pins (col.5, lines 5-10 and 38-42). The virtual key can obviously be Kanevsky's password (or gesture pin) that is used to verify the person or user to gain access to the building or facilities (col.5, lines 40-43 and col.8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col.17, lines 5-7). Therefore, the gesture pin is transmitted to the user (col.17, lines 6-7) for use to access the facility/service prompting checking the validity of the gesture pin against the stored ones of a database (col.15, lines 41-47 and 18, lines 8-24). So depending on the security task(s) involved and the results of the user evaluation, the user is either granted/denied access to a service/facility or

confirmed/denied with respect to ownership of an item (proof of possession, or information pertaining to the user's biometrics will be stored in a user database for different applications (col.8, lines 5-12 and col.12, lines 37-48). Thus, checking the validity of the gesture pin (of h-i) has to involve a pre-stored gesture pin in order for use to compare if the validity check is positive after the generated/produced gesture pin is transmitted to the user (col.17, lines 6-7).

An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords and the password is a virtual key that authenticates a user (col.1, lines 43-48 and col.2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art combine Kanevsky and An to teach the virtual key refers to a password (gesture pin) because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to allow access to something (i.e. building or facilities).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100